$ AF
CFW

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Appellants:	**Arindam Das-PURKAYASTHA et al.**	Examiner:	Longbit CHAI
Serial No.:	**09/931,526**	Art Unit:	2131
Filed:	August 16, 2001	Our Ref:	30006636-3 US
For:	"APPARATUS AND METHOD FOR ESTABLISHING TRUST"	Date:	August 2, 2005
		Re:	***Appeal to the Board of Appeals***

BRIEF ON APPEAL

Mail Stop Appeal Brief - Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

8

Sir:

This is an appeal from the Final rejection, dated March 29, 2005, for the above identified patent application. Please charge the amount of $500.00 for the fee set forth in 37 C.F.R. 1.17(c) for submitting this Brief to deposit account no. 08-2025. Appellants submit that this Appeal Brief is being timely filed, since the notice of Appeal was filed on June 28, 2005.

REAL PARTY IN INTEREST

The real party in interest to the present application is Hewlett-Packard Development Company, LP, a limited partnership established under the laws of the State of Texas and having a principal place of business at 20555 S.H. 249 Houston, TX 77070, U.S.A. (hereinafter "HPDC"). HPDC is a Texas limited partnership and is a wholly-owned affiliate of Hewlett-Packard Company, a Delaware Corporation, headquartered in Palo Alto, CA. The general or managing partner of HPDC is HPQ Holdings, LLC.

STATUS OF CLAIMS

Claims 1 - 61 are the subject of this Appeal and are reproduced in the accompanying appendix.

STATUS OF AMENDMENTS

No Amendment After Final Rejection has been entered.

SUMMARY OF THE INVENTION

The invention described and claimed in the present application relates generally to computer security, and more specifically to the establishment of a particular level of trust in a computer based upon the response of that computer to a challenge. Key to the present invention is the existence of a physically trusted device within the computer, that is, a device that is tamper-proof, and that is able to acquire and provide an integrity metric for the computer in response to a challenge (p. 5, ll. 3-8). The integrity metric provided by the trusted device is then compared with an integrity metric for the computer that is provided by a trusted party, and the challenger decided upon a level of trust to place in the computer based upon whether the two integrity metrics match, and optionally the scope of the integrity metric (p. 5, ll. 9-10). The integrity metric has values for a plurality of characteristics associated with the computer (claim 1), such as a digest of the BIOS instructions in the BIOS memory of the computer (p. 10, ll. 10-12). Preferably each component, but at least each critical component, of the computer has an integrity value associated with it, a so-called CCV (Component Configuration Value), that can be included in the integrity metric acquired by the trusted device of the computer (p. 10, l. 22 p. 11, l. 7). There are a number of ways the integrity metric may be calculated, all of which are contemplated by the invention (p. 15, l. 16 – p. 16, l. 32).

ISSUES

Issue 1: Whether claims 1, 2 and 6 are patentable under 35 U.S.C. 103(a) over U.S. Pat. No. 6,009,177 to Sudia (hereinafter "Sudia") in view of U.S. Pat. No. 6,430,561 to Austel (hereinafter "Austel") and ISO/IEC-15408.

Issue 2: Whether claims 3-5 are patentable under 35 U.S.C. 103(a) over Sudia in view of Austel and in view of U.S. Pat. No. 5,919,257 to Trostle (hereinafter "Trostle").

Issue 3: Whether Claims 7-61 are directed to an invention that is independent or distinct from the invention claimed in claims 1-6.

GROUPING OF CLAIMS

For each ground of rejection which Appellants contest herein and which applies to more than one claim, such additional claims, to the extent separately identified and argued below, do not stand or fall together.

THE ARGUMENT

Issue 1: Whether claims 1, 2 and 6 are patentable under 35 U.S.C. 103(a) over U.S. Pat. No. 6,009,177 to Sudia (hereinafter "Sudia") in view of U.S. Pat. No. 6,430,561 to Austel (hereinafter "Austel") and ISO/IEC-15408.

On page 4, section 1 of the Office Action of March 29, 2005, the Examiner rejects Claims 1, 2 and 6 under 35 U.S.C. 103(a) as being unpatentable over Sudia in view of Austel and as evidenced by ISO/IEC-15408. In particular, the Examiner opines in section 2 that with regard to claims 1 and 6, Sudia teaches computer apparatus comprising a receiver for receiving an integrity metric for a computer entity via a trusted device associated with the computer entity, the integrity metric having values for a plurality of characteristics associated with the computer. In

support of this proposition, the Examiner cites to Sudia, col. 16 ll. 50-67, col. 44 ll. 31-55, and elements 240/241/248 in Fig. 24. Appellants respectfully disagree with the Examiner's understanding and characterization of this reference.

As clearly and carefully laid out in Appellants' submission of December 9, 2004, Sudia contains no teachings or allusions to the use of an integrity metric as claimed. Sudia generally relates to a chip device that acts as a trusted device for the user and that contains a number of secrets, some of which may be externally disclosed and some not (see, e.g., col. 16, l. 9 to col. 17, l. 27). None of these secrets are described as being a measurement relating to the integrity of the trusted device or of a computing entity to which it relates, and therefore none of these secrets are, or are capable of performing the function of, an integrity metric as claimed. The portion of the specification cited to by the Examiner at col. 16 ll. 50-67 states:

> This scheme can also apply to firmware code routines just as easily as to data, and may be advantageously applied when upgrading or replacing trusted firmware code routines without needing to physically replace the device or any of its memory units.
>
> The protected memory areas of a device of a preferred embodiment of the present invention might contain the following types of information, including both data and firmware program code.
>
> A. Permanently Embedded by Manufacturer
>
> 1. May Be Externally Disclosed
>
> a. system-wide authority public key (optional)
>
> b. manufacturer public key
>
> c. manufacturer certificate from system-wide authority
>
> d. device public key
>
> e. device certificate from manufacturer

f. device unique serial number

g. firmware version numbers

h. trusted bank public instruction keys

The portion of the specification cited to by the Examiner at col. 44 ll. 31-55 states:

When satisfied that the user can be permitted to engage in the requested class of transactions, the TTP 241 then issues a response 246 containing a certificate 247 specifically authorizing the device to perform those transactions on behalf of the user. The TTP's device authorization certificate 247 will typically contain information identifying the TTP, the user, the user's device, and the transactions for which permission is granted, as well as a recertified copy of the user's device public signature key as a matter of convenience (and as later discussed) so that the user need not submit his device certificate 242 in each subsequent transaction with trading partners. The TTP response 246 may also contain downloadable firmware and or public keys 248 to be loaded into the user's trusted device to enable it to perform the authorized transactions. Where the TTP response 246 calls for the user to securely load new firmware or public keys into his device, the response 246 will also include the TTP's certificate of authority 243 issued by the SWA certifying the TTP's public signature key and conveying firmware and public key upgrade authority. When the user's trusted device 240 receives the TTP's response 246, it uses its embedded SWA public signature key to verify the TTP's certificate of authority 243 and uses the TTP public

> signature key contained therein to verify the firmware and public key upgrades 248 and the TTP's device authorization certificate 247.

The above describes part of what is shown in Fig. 24, also cited to by the Examiner.

A very careful reading of the portions of the Sudia specification reproduced above fails to disclose or allude to the use of an integrity metric having values for a plurality of characteristics associated with a computer entity. This was made abundantly clear in Appellant's previous response, wherein a discussion and explanation of Sudia's actual disclosure was presented. As previously explained, Sudia clearly shows in Figure 24 and in the related text at col. 43 l. 54 to col. 45 l. 57 that the trusted device of Sudia interacts with a trusted third party to receive permission to conduct certain classes of transactions (col. 43, l.54 – col. 45, l. 57) such that the trusted third party can obtain "some information to identify the user and the nature of the registration request" and "other information and assurances from either the user or from other parties to verify the user's identity, affiliation, creditworthiness, etc." (col. 44, ll. 14-29) to determine whether this permission can be granted. If permission can be granted, the trusted third party provides an appropriate certificate, possibly accompanied by downloadable firmware and keys (col. 44, ll. 30-55, also cited to by the Examiner). Information verifying the user's identity, affiliation, creditworthiness, etc. is certainly not, nor an equivalent to, an integrity metric having values for a plurality of characteristics associated with a computer entity. The disclosure at column 16, lines 5-67 cited to by the Examiner contains merely a recitation of information that may be permanently embedded by a manufacturer into a protected memory area of a device. This too cannot possibly be read as corresponding to an integrity metric having values for a plurality of characteristics associated with a computer entity as claimed and further described in the specification of the application.

In the final Action, the Examiner dismisses all of the above by stating that the "Examiner notes the integrity metric is interpreted as the value that can enforce the desired level of protection (i.e. authentications) such as the device unique serial number, firmware version number, device private signature key (Saudi: see for example, Column 16 Line 45 – Column 17 Line 7 and Figure 24 Element 240); and this trust device is associated a computer entity (Saudi:

see for example, Column 7 Line 45 – 47). Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993)." The Examiner gratuitous citation to In re Van Geuns notwithstanding, Appellants nonetheless note that their entire argument is based upon the lack of disclosure in Sudia of a limitation that is very clearly and expressly already present in the claims, namely an "integrity metric having values for a plurality of characteristics associated with the computer entity." The Examiner's puzzling decision to interpret "integrity metric" as something very clearly at odds with the specific definition laid out in the independent claims, i.e. as "having values for a plurality of characteristics associated with the computer entity" is unsupported, impermissible, and plain wrong.

Appellants further respectfully submit that the Examiner's assertion that an integrity metric is "the value that can enforce the desired level of protection (i.e. authentications)" is also devoid of merit. A value enforces nothing, it is merely a number. Furthermore, there is absolutely no disclosure in Sudia of the trusted device or any other device using values such as "the device unique serial number, firmware version number" for the purpose of selecting a level of trust, or for simply authenticating. While Sudia does disclose using a device private signature key for authentication purposes, such a key is clearly not a value for a *characteristic associated with the computer entity*. The Examiner appears to not appreciate the fundamental differences between Sudia and the Appellant's invention, namely the assigning of trust based upon the integrity of the computer. Sudia, on the other hand, is concerned with *cryptographic communications* and the use of a trusted device that self-certifies (please see col. 1, ll. 14-20), that is, the encryption chip is capable of proving that it is to be trusted because it contains a private signature key that is embedded into it in a tamper-resistant manner (see, *e.g.*, col. 13, ll. 11-21). The trusted device of Sudia, i.e. the encryption chip, does not inquire into characteristics of the computer and does not acquire values for these characteristics into an integrity metric to be provided in response to a challenge to the computer.

Appellants further traverse the Examiner's assertion that Austel discloses "assigning a trust level to the computer entity from a plurality of trust levels, wherein the assigned trust level is based upon the value of at least one of the characteristics of the received integrity metric." As previously explained by Appellants, Austel is directed to a method for implementing a security

policy for controlling access by programs to protected files. The method of Austel assigns access classes to files and to accessing programs, and allows files to be accessed and operated on only in accordance with an appropriate set of rules. Each access class includes an integrity access class and a secrecy access class, each comprising rules for read, write and execute functions. One embodiment is described as assigning the integrity access class "based on the results of an independent external evaluation process" such as ITSEC and EAL (col. 10, ll. 44-58). There is absolutely no disclosure in Austel of anything akin to calculating an integrity metric as recited in the claims. The Examiner appears to assume that, because Austel terms one of the classes an "integrity access class," it is the same as the integrity metric of the present claims. This is simply not supported by the plain language of Austel.

In the final Action, the Examiner retorts to the above by noting on page 4 that "Saudi is relied upon to provide the integrity metric and Austel is relied upon assigning integrity access class (i.e. trust level) through an independent external evaluation process which is selected from the group consisting of Common Criteria EAL levels." This is entirely self contradictory, as it completely negates the Examiner's own assertion at page 5, section 4, that "Austel teaches a controller for assigning a trust level to the computer entity from a plurality of trust levels, wherein the assigned trust level is based upon the value of at least one of the characteristics of the received integrity metric." The Examiner's flip-flopping aside, the disclosure of Austel clearly does not fill in the gaps in the Sudia document. In view of all of the preceding, Appellants respectfully submit that claims 1 and 6 are in fact novel and nonobvious over the cited art, and request that the Examiner's rejection of these claims be overturned on appeal.

Claim 2 depends from claim 1. "If an independent claim is nonobvious under 35 U.S.C. 103, then any claim depending therefrom is nonobvious." *In re Fine*, 837 F.2d 1071, 5 USPQ2d 1596 (Fed. Cir. 1988). Therefore, in view of the above discussion, it is submitted that claim 1 is allowable, and for this reason claim 2 is also allowable.

Issue 2: Whether claims 3-5 are patentable under 35 U.S.C. 103(a) over Sudia in view of Austel and in view of U.S. Pat. No. 5,919,257 to Trostle (hereinafter "Trostle").

On page 6, section 8 of the Office Action of March 29, 2004, the Examiner rejects claims 3-5 under 35 U.S.C. 103(a) as being unpatentable over Sudia in view of Austel and in view of Trostle.

Claims 3-5 depend from claim 1. Therefore, in light of the above discussion of claim 1, Appellants submit that claims 3-5 are also allowable.

Issue 3: Whether Claims 7-61 are directed to an invention that is independent or distinct from the invention claimed in claims 1-6.

On page 2, section 2 of the Office Action of March 29, 2004, the Examiner asserts that Claims 7-61 are directed to an invention that is independent or distinct from the invention claimed in claims 1-6. The Examiner opines that claims 7-61 disclose a method of deriving an integrity metric and belong in class 713/161, whereas original claims 1-6 disclose a method of using the value of the integrity metric and belong to class 713/200. The Examiner thus appears to find the claims independent and distinct because they are related as subcombinations that can be shown to be separately usable. However, the Examiner fails to take the last, all-important step of actually making such a showing that these subcombinations are separately usable. The Examiner's bland assertion that the two groups of claims belong in different subclasses of the same class does not amount to a sufficient showing under the rules. Appellants further contend that the inventions claimed in these two groups of claims are not in fact separately usable – they are both directed to the assignment of a trust level to a computer based upon an integrity metric of that computer. Claims 1-6 are directed to a computer apparatus for assigning such a trust level, whereas claims 7-61 are directed to a method for assigning such a trust level. The Examiner's assertion that these are "separately usable" is without merit – how can a method for assigning a trust level to a computer based upon an integrity metric of that computer be "separately usable" from a computer implementing

a method for assigning a trust level to a computer based upon an integrity metric of that computer?

Appellants respectfully traverse the Examiner's restriction and respectfully request the Board to reinstate claims 7-61 on appeal.

CONCLUSION

In view of the extensive reasons advanced above, Appellants respectfully contend that each claim is in fact novel and patentable. Therefore, reversal of all rejections and objections and re-opening of the prosecution is respectfully solicited.

I hereby certify that this correspondence is being deposited with the United States Post Service with sufficient postage as first class mail in an envelope addressed to: Mail Stop Appeal Brief-Patents, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on

August 2, 2005
(Date of Transmission)

Mia Kim
(Name of Person Transmitting)

(Signature)

8/2/05
(Date)

Respectfully submitted,

Robert Popa
Attorney for Appellant
Reg. No. 43,010
LADAS & PARRY
5670 Wilshire Boulevard, Suite 2100
Los Angeles, California 90036
(323) 934-2300 voice
(323) 934-0202 facsimile
rpopa@ladasparry.com

Attachments

Claims

1. (previously presented) Computer apparatus, comprising:

a receiver for receiving an integrity metric for a computer entity via a trusted device associated with the computer entity, the integrity metric having values for a plurality of characteristics associated with the computer entity; and

a controller for assigning a trust level to the computer entity from a plurality of trust levels, wherein the assigned trust level is based upon the value of at least one of the characteristics of the received integrity metric.

2. (original) Computer apparatus according to claim 1, wherein the trusted device is arranged to acquire an integrity metric of the computer entity.

3. (original) Computer apparatus according to claim 1, wherein the trust level is determined by comparing the value of the at least one characteristics with a specified value.

4. (original) Computer apparatus according to claim 1, wherein the plurality of trust levels are determined base upon a plurality of specified values associated with a plurality of characteristics of a computer entity.

5. (original) Computer apparatus according to claim 1, wherein the plurality of trust levels are determined based upon a plurality of specified values associated with characteristics for a plurality of computer entities.

6. (previously presented) A method of assigning a trust level, comprising:

receiving an integrity metric for a computer entity via a trusted device associated with the computer entity, the integrity metric having values for a plurality of characteristics associated with the computer entity; and

assigning a trust level to the computer entity from a plurality of trust levels, wherein the assigned trust level is based upon the value of at least one of the characteristics of the received integrity metric.

7. (previously presented) A method for establishing communications with a computer entity, comprising:

requesting a trusted device associated with a computer entity to provide an integrity metric calculated for the entity by the trusted device and containing values indicative of one or more characteristics of the entity;

receiving a response from the trusted device including an integrity metric calculated for the entity by the trusted device;

comparing values in the integrity metric calculated for the entity by the trusted device with authenticated values provided for the entity by a trusted party; and

selecting a level of trust for the entity from a plurality of predefined levels of trusts based on at least one value in the integrity metric calculated for the entity by the trusted device.

8. (previously presented) The method of claim 7, wherein the trusted device is hardwired to the computer entity.

9. (previously presented) The method of claim 8, wherein the trusted device is configured to control the boot process of the computer entity.

10. (previously presented) The method of claim 9, wherein the trusted device is configured to not respond to the request for the integrity metric if the boot process of the computer entity was not controlled by the trusted device.

11. (previously presented) The method of claim 8, wherein the trusted device is comprised of a plurality of components hardwired to the computer entity.

12. (previously presented) The method of claim 7, wherein the trusted device is configured to contain one or more of a public encryption key, a private encryption key, and one or more authenticated values provided for the entity integrity metric by the trusted party.

13. (previously presented) The method of claim 12, wherein the trusted device is configured to calculate the integrity metric by generating a digest of BIOS instructions in the BIOS memory of the entity.

14. (previously presented) The method of claim 12, wherein the trusted device is configured to calculate the integrity metric by measuring one or more values of configuration information regarding one or more components of the entity.

15. (previously presented) The method of claim 14, wherein the components of the entity are selected from among the group

of components comprising hardware components and software components.

16. (previously presented) The method of claim 15, wherein the components of the entity are selected from among the group of components comprising the BIOS, ROM, operating system loader, and operating system of the entity.

17. (previously presented) The method of claim 15, wherein the configuration information measured for at least one of the components comprises one or more of certificate information, last update information, latest update version information, and previous update information.

18. (previously presented) The method of claim 12, wherein the trusted device is configured to calculate the integrity metric by engaging in predetermined interactions with one or more components of the entity and acquiring the values of the responses of the one or more components.

19. (previously presented) The method of claim 12, wherein the response received from the trusted device includes the authenticated values provided by the trusted party.

20. (previously presented) The method of claim 7, wherein requesting the trusted device for the integrity metric comprises:

generating a nonce to pass to the trusted device with the request.

21. (previously presented) The method of claim 20, wherein

the response from the trusted device includes the nonce received with the request.

22. (previously presented) The method of claim 7, further comprising:

initiating data transfer to the entity in accordance with the selected trust level.

23. (previously presented) The method of claim 22, wherein initiating data transfer to the entity in accordance with the selected trust level comprises transferring no data.

24. (previously presented) A method for a computer entity to respond to a request for integrity check prior to exchanging data, comprising:

receiving at a trusted device associated with a computer entity a request to provide an integrity metric containing values indicative of one or more characteristics of the entity;

calculating at the trusted device values indicative of one or more characteristics of the entity; and

providing a response from the trusted device including an integrity metric including the values indicative of one or more characteristics of the entity.

25. (previously presented) The method of claim 24, wherein the trusted device is hardwired to the computer entity.

26. (previously presented) The method of claim 25, wherein the trusted device is configured to control the boot process of the computer entity.

27. (previously presented) The method of claim 25, wherein the trusted device is configured to not respond to the request for the integrity metric if the boot process of the computer entity was not controlled by the trusted device.

28. (previously presented) The method of claim 25, wherein the trusted device is comprised of a plurality of components hardwired to the computer entity.

29. (previously presented) The method of claim 24, wherein the trusted device is configured to contain one or more of a public encryption key, a private encryption key, and one or more authenticated values provided for the entity integrity metric by the trusted party.

30. (previously presented) The method of claim 29, wherein the integrity metric includes one or more values calculated by generating a digest of BIOS instructions in the BIOS memory of the entity.

31. (previously presented) The method of claim 29, wherein the trusted device is configured to calculate the integrity metric by measuring one or more values of configuration information regarding one or more components of the entity.

32. (previously presented) The method of claim 31, wherein the components of the entity are selected from among the group of components comprising hardware components and software components.

33. (previously presented) The method of claim 32, wherein

the components of the entity are selected from among the group of components comprising the BIOS, ROM, operating system loader, and operating system of the entity.

34. (previously presented) The method of claim 32, wherein the configuration information measured for at least one of the components comprises one or more of certificate information, last update information, latest update version information, and previous update information.

35. (previously presented) The method of claim 29, wherein the trusted device is configured to calculate the integrity metric by engaging in predetermined interactions with one or more components of the entity and acquiring the values of the responses of the one or more components.

36. (previously presented) The method of claim 35, wherein the components of the entity are selected from among the group of components comprising hardware components and software components.

37. (previously presented) The method of claim 29, wherein the response further includes authenticated values provided for the entity by a trusted party.

38. (previously presented) The method of claim 29, wherein the request includes a nonce.

39. (previously presented) The method of claim 38, wherein the response includes the nonce received with the request.

40. (previously presented) The method of claim 29, wherein the request includes input data.

41. (previously presented) The method of claim 40, wherein the response includes the input data processed with the private encryption key.

42. (previously presented) A method for establishing communications between a computer entity and a user, comprising:

presenting a request from the user to a trusted device associated with a computer entity to provide an integrity metric calculated for the entity by the trusted device and containing values indicative of one or more characteristics of the entity;

presenting to the user a response from the trusted device including an integrity metric calculated for the entity by the trusted device;

comparing at the user values in the integrity metric calculated for the entity by the trusted device with authenticated values provided for the entity by a trusted party; and

selecting at the user a level of trust for the entity from a plurality of predefined levels of trusts available to the user based on at least one value in the integrity metric calculated for the entity by the trusted device.

43. (previously presented) The method of claim 42, wherein the trusted device is hardwired to the computer entity.

44. (previously presented) The method of claim 43, wherein the trusted device is configured to control the boot process of the computer entity.

45. (previously presented) The method of claim 44, wherein the trusted device is configured to not respond to the request for the integrity metric if the boot process of the computer entity was not controlled by the trusted device.

46. (previously presented) The method of claim 43, wherein the trusted device is comprised of a plurality of components hardwired to the computer entity.

47. (previously presented) The method of claim 42, further comprising:
passing from the trusted party to the trusted device one or more of a public encryption key, a private encryption key, and one or more authenticated values for the entity integrity metric.

48. (previously presented) The method of claim 47, wherein the trusted device is configured to calculate the integrity metric by generating a digest of BIOS instructions in the BIOS memory of the entity.

49. (previously presented) The method of claim 47, wherein the trusted device is configured to calculate the integrity metric by measuring one or more values of configuration information regarding one or more components of the entity.

50. (previously presented) The method of claim 49, wherein the components of the entity are selected from among the group of components comprising hardware components and software components.

51. (previously presented) The method of claim 50, wherein the components of the entity are selected from among the group of components comprising the BIOS, ROM, operating system loader, and operating system of the entity.

52. (previously presented) The method of claim 50, wherein the configuration information measured for at least one of the components comprises one or more of certificate information, last update information, latest update version information, and previous update information.

53. (previously presented) The method of claim 47, wherein the trusted device is configured to calculate the integrity metric by engaging in predetermined interactions with one or more components of the entity and acquiring the values of the responses of the one or more components.

54. (previously presented) The method of claim 49, wherein the components of the entity are selected from among the group of components comprising hardware components and software components.

55. (previously presented) The method of claim 47, wherein the response received from the trusted device includes the authenticated values provided by the trusted party.

56. (previously presented) The method of claim 42, wherein the request includes a nonce.

57. (previously presented) The method of claim 56, wherein the response includes the nonce received with the request.

58. (previously presented) The method of claim 47, wherein the request includes input data.

59. (previously presented) The method of claim 58, wherein the response includes the input data processed with the private encryption key.

60. (previously presented) The method of claim 42, further comprising:

initiating data transfer from the user to the entity in accordance with the selected trust level.

61. (previously presented) The method of claim 60, wherein initiating data transfer from the user to the entity in accordance with the selected trust level comprises transferring no data.